Deutscher Bundestag **Drucksache 17/8277**

17. Wahlperiode 29. 12. 2011

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan Korte, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 17/8145 –

Polizeiliche Soft- und Hardware bei den EU-Agenturen

Vorbemerkung der Fragesteller

Seit Jahren rüsten auch polizeiliche EU-Agenturen ihr digitales Arsenal auf. Europol (Europäisches Polizeiamt) will zum „weltweit herausragenden Zentrum der Weltklasse“ (world-class centre of excellence) werden, was sich vor allem auf den IT-Bereich bezieht (www.europol.europa.eu/sites/default/files/publications/anniversary_publication.pdf). Zentraler Bestandteil von Europol sind die umfangreichen Datenbanken, deren Einrichtung im Europol-Übereinkommen festgelegt ist. Das „automatisierte System“ besteht aus drei Säulen, dem Informationssystem, den Analysedateien und einem Indexsystem. Etliche EU-weite Abkommen erweitern die Zugriffsmöglichkeiten der Behörde. Europol selbst bezeichnet sich als „Information-Broker“ und sieht sich dem Grundsatz eines „proaktiven Handelns“. Mit dem deutschen Jürgen Storbeck als ersten amtierenden Direktor 1999 und seinem Nachfolger Max-Peter Ratzel, vorher Abteilungspräsident des Bundeskriminalamts (BKA), konnte Deutschland bis zum Antritt des britischen Rob Wainwright 2009 sein Gewicht in der Organisation ausbauen. Max-Peter Ratzel hatte im Oktober 2007 die neue „Strategy for Europol“ vorgestellt. Durch die Ausweitung analytischer Kapazitäten sollte die Behörde zum Pionier des „Wandels, Identifizierung und Antwort auf neue Bedrohungen und der Entwicklung neuer Technik“ werden. Auch bei Europol kommt Software zur Vorgangsverwaltung, zu Ermittlungs- oder Analysezwecken oder zum Data-Mining zur Anwendung. Nicht nur der Abgleich mehrerer Datensätze ist dabei problematisch und kann als „Profiling“ bezeichnet werden. Die Software kann zudem mit „Zusatzapplikationen“ oder „Modulen“ erweitert werden, um weitere Datenbanken oder das Internet über Schnittstellen einzubinden. Im jüngsten Europol Review wirbt die Agentur mit einer „state-of-the-art facility to extract and analyse crime-related information from digitised data“. Unter deutscher Federführung arbeitet bei Europol ein „Mobile Competence Team“ (MCT) unter anderem zur Umsetzung des Vertrags von Prüm zum grenzüberschreitenden Datentausch.

Eines der „Angebote“ der Agentur ist das „24/7 operational centre“, das Daten aus gemeinsamen Operationen von Polizeien der Mitgliedstaaten der Europäischen Union (EU) mit anderen Datensätzen abgleicht (incoming data are quickly cross-checked against all existing data). Die mobile Einheit errichtet eine „live

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 28. Dezember 2011 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

connection“ zur Agentur. Genutzt wird die Plattform anscheinend auch für politische Proteste oder Sportereignisse (internationally prominent sporting, economic, political or cultural gatherings). Zur Analyse von Netzwerken nutzt Europol ein „SNA tool“, das angeblich bei einer einzigen Aktion (Operation Most) 25 Verdächtige aus einer Million von polnischen Behörden mitgeschnittenen Telefongespräche präsentierte. Europol verfügt außerdem über weitere „forensische Ausrüstung“, etwa das „forensic toolkit“ (UFED) oder „mobile phone scanners“. Als bewegliche Einheit fungiert ein „expert-operated mobile toolkit for computer data forensics“. Zudem koordiniert Europol ein „Computer Forensic Network“. Bislang unbekannte Methoden und Anwendungen werden innerhalb einer „Cross-Border Surveillance Working Group“ (CSW) erörtert, deren Mitglied Europol ist.

Auch die Europäische Agentur für die operative Zusammenarbeit an den Außengrenzen FRONTEX stattet seine Zentrale in Warschau mit Soft- und Hardware aus. FRONTEX betreibt eine „Situation Center Unit“, um „Risikoanalysen“ oder Lageberichte zu verfassen. Als Nutzeroberfläche entwickelte die Agentur das Frontex One-Stop-Shop web portal (FOSS), an das zunehmend Behörden der EU-Mitgliedstaaten angeschlossen werden und das später das EU-weite Überwachungssystem EUROSUR (Europäisches Grenzkontrollsystem) verwaltet. Weitere digitale Plattformen sind ein „Frontex Media Monitor“ oder die „Joint Operations Reporting Application” (JORA). Hinzu kommen zahlreiche weitere Datenbanken oder Netzwerke, die zunehmend mit digitaler Analysekapazität aufgerüstet werden. Ein „European Network of Law Enforcement Technology Services“ (ENLETS) soll den Erfahrungsaustausch zu digitaler Überwachung EU-weit verbessern und ein Register zu „Sicherheitstechnologie“ anlegen.

Über die Funktionsweise der beschriebenen Anwendungen ist wenig bekannt. Es besteht die Möglichkeit, über den Sachverstand, aber auch die technische Ausrüstung von EU-Agenturen, bestehende nationale Beschränkungen zu umgehen. Die Geschwindigkeit, mit der etwa Europol zum führenden IT-Dienstleister in der Kriminaltechnik avanciert, steht in keinem Verhältnis zur öffentlichen Debatte, inwieweit diese Entwicklung von der Bevölkerung akzeptiert wird. Die digitale Aufrüstung ist nicht verhältnismäßig. Auch ihre Notwendigkeit kann nicht bewiesen werden. Es profitieren indes die großen Rüstungs- und Softwarekonzerne. Wirtschaftliche Argumente zur Ausweitung digitaler Kriminaltechnik, etwa das Einsparen von Beamtinnen und Beamten, führen zur Aushöhlung von Bürger- und Bürgerinnenrechten. Bürgerrechtlerinnen und Bürgerrechtler, netzpolitische Aktivistinnen und Aktivisten, Anwältinnen und Anwälte, soziale Bewegungen und Parlamentarierinnen bzw. Parlamentarier müssen einen Einblick in die Funktionsweise der Anwendungen erlangen. Das Konzept einer informationstechnischen „Überlegenheit auf allen Ebenen“ ist dem Militär entlehnt. Die zunehmend „vorausschauende“ digitale Überwachung setzt die Unschuldsvermutung außer Kraft. Risikoanalysen geraten zum Profiling, wenn auf mehrere Datensätze zugegriffen werden kann. Dieser Prozess ist zudem auf Wachstum angelegt: Statistische Verfahren in der Polizeiarbeit sind auf stets erweiterte und erneuerte Datensätze angewiesen, um „Prognosen“ zu verbessern.

Vorbemerkung der Bundesregierung

Die Beantwortung der Anfrage erfordert fundierte Kenntnisse des internen Betriebs und der internen technischen Infrastruktur von Europol, über die die Bundesregierung nur teilweise verfügt. Die parlamentarische Kontrolle über Europol wird durch das Europäische Parlament ausgeübt. Die technischen Arbeitsgruppen bei Europol unter Beteiligung der Mitgliedstaaten befassen sich mit diesen agenturinternen betrieblichen Fragestellungen nicht. Dort werden vielmehr fachliche, organisatorische und finanzielle Fragen beraten. Technische Details werden nur dann erörtert, wenn nationale Implementierungen in den Mitgliedstaaten betroffen sind.

Daher wurden den Mitgliedstaaten auch bisher keine Dokumente, die Detailinformationen über den technischen Betrieb und die technische Infrastruktur von Europol betreffen, übermittelt und zur Verfügung gestellt. Entsprechende Kenntnisse liegen der Bundesregierung daher nicht vor. Insofern kann eine Anzahl der Teilfragen nicht beantwortet werden.

Nur die bei Europol beschäftigten Analytiker sind befugt, Daten in die jeweilige Analysedatei nach Artikel 14 des Europol-Ratsbeschlusses (Beschluss des Rates vom 6. April 2009 zur Errichtung des Europäischen Polizeiamts (Europol) 2009/371/JI) einzugeben und diese Daten zu ändern. Der Bundesregierung liegen daher keine detaillierten Informationen über die technische Ausgestaltung der Analysedateien vor.

1. Welche computergestützten Analysewerkzeuge kommen bei welchen Abteilungen der EU-Polizeiagentur Europol zum Einsatz?

Europol verwendet im Bereich der Analyse Werkzeuge zur Unterstützung der einzelnen Arbeitsschritte und Prozessabläufe. Dies betrifft die Dateneinstellung, die Aufbereitung der Daten und die Erstellung von Berichten bzw. die Datenausgabe. Hierbei werden die Möglichkeiten von Dokumenten Management Systemen, des Text- und Data Minings sowie der webbasierten Datenvisualisierung und Übersetzungstools eingesetzt. Die hierzu vom Markt gekauften Produkte werden von Europol durch eigene Entwicklungen ergänzt und so zu Workflows zusammengefügt. Die von Europol verwendeten Produkte und die dahinter stehenden Firmen sind im Einzelnen der Bundesregierung nicht bekannt. Aufgrund der Organisationsstruktur von Europol werden die Analysewerkzeuge fachlich durch die Abteilung „Operations“ genutzt.

Der Betrieb, die Integration der Produkte in die Prozessabläufe sowie der Support erfolgt durch die Abteilung „Capabilities“.

a) Auf welcher Hardware welcher Firmen basieren die Informationssysteme der EU-Agentur (auch Serversysteme und Netzwerke)?

Europol verwendet mehrere Netzwerke, die über unterschiedliche Sicherheitsstandards verfügen. Alle Netzwerke sind voneinander getrennt. Die Kernanwendungen von Europol werde über das Europol Secure Network betrieben. Für die sichere Kommunikation mit den Mitgliedstaaten wird das europäische sTESTA Netzwerk verwendet. Die Übertragung von Daten erfolgt verschlüsselt.

Details über die von Europol verwendete Hardware liegen der Bundesregierung nicht vor.

b) Welche Software welcher Hersteller kommt für welche Bereiche zum Einsatz als

aa) Vorgangsverwaltung,

bb) Ermittlungssoftware,

cc) Analysesoftware,

dd) Data-Mining,

ee) Bildersuche?

Im Hinblick auf die Europol Schlüssel-Applikationen (Europol Informationssystem (EIS), Europol Analysis System (EAS) und Secure Information Exchange Network Application (SIENA)) verwendet Europol vorwiegend Eigenentwicklungen. Wie unter Frage 1 ausgeführt, können in bestimmten Teilbereichen kommerzielle Produkte zur Unterstützung eingesetzt werden, diese

werden jedoch in die Europol Umgebung eingepasst. Detaillierte Informationen über diese Produkte und Namen von Herstellern liegen der Bundesregierung nicht vor.

c) Mit welchen „Zusatzapplikationen“ oder „Modulen“ ist die Software ausgestattet, um etwa weitere Datenbanken oder das Internet über Schnittstellen einzubinden?

Hierzu liegen der Bundesregierung keine Informationen vor.

d) Welche weiteren Zusatzmodule können für die Software erworben werden, und welche Überlegungen finden hierzu statt?

Hierzu liegen der Bundesregierung keine Informationen vor.

e) Auf welche Datenbanken können welche Anwendungen im Einzel- und im Regelfall jeweils zugreifen?

Es ist der Bundesregierung nicht bekannt, welche Anwendungen auf einzelne Datenbanken zugreifen können. Im Regelfall werden die Datenbanken des EIS und des EAS mit den dort enthaltenen Analytical Work Files (AWFs) abgefragt.

2. Welche technischen Kapazitäten im Bereich von Telekommunikationsüberwachung werden vom „24/7 operational centre“ der EU-Agentur Europol entwickelt und angeboten?

Detaillierte Informationen zum „24/7 operational centre“ liegen der Bundesregierung nicht vor. Der Bundesregierung wurden bisher auch keine technischen Kapazitäten oder Entwicklungen aus dem Bereich Telekommunikations-Überwachung angeboten.

a) Nach welchen technischen Verfahren können im „24/7 operational centre“ eingehende Daten aus gemeinsamen Operationen von Polizeien der EU-Mitgliedstaaten mit anderen Datensätzen abgeglichen werden (incoming data are quickly cross-checked against all existing data)?

Hierzu liegen der Bundesregierung keine Informationen vor.

b) Welche Datenbanken der EU-Agentur oder andere Datensammlungen können derart abgefragt werden, und wie ist dies rechtlich geregelt?

Folgende Systeme können abgefragt werden:

- Europol Analysis System mit den dort enthaltenen Analytical Work Files (AWFs),
- Europol Information System (EIS).

Rechtlich geregelt sind die Abfragemöglichkeiten in Artikel 13 und 14 des Europol-Ratsbeschlusses vom 6. April 2009 (2009/371/JHA).

c) Wie und wohin werden gefundene „Treffer“ ausgegeben?

Erzielte Treffer werden schriftlich auf dem Kooperationskanal von Europol an die in Bezug auf den Treffer betroffenen Staaten übermittelt. Die Informationen müssen dabei im Einklang mit den Zweckbindungsklauseln stehen.

d) Auf welche Weise wird ein weitergehender Bericht (one analytical report) für derartige Operationen ausgefertigt, bzw. welche Daten liegen diesem zugrunde?

Weitergehende Berichte werden ebenfalls schriftlich auf Basis der für den jeweiligen Bericht relevanten Daten erstellt.

e) Welche Rolle spielt das „24/7 operational centre“ in der Koordination „polizeilicher Großlagen“ bzw. welche Überlegungen werden hierzu angestellt?

Detaillierte Informationen zum „24/7 operational centre“ liegen der Bundesregierung nicht vor.

3. Wie wird die „live connection“ technisch umgesetzt, die Europol im Rahmen seines „24/7 operational centres“ für grenzüberschreitende Operationen anbietet?

Der Begriff „live connection“ und das dahinter stehende Verfahren wurde in den Europol internen Arbeitsgruppen, an denen die Mitgliedstaaten beteiligt sind – ICT Working Group und Security Committee – nicht vorgestellt oder erörtert. Detailkenntnisse liegen der Bundesregierung daher nicht vor.

a) Welche Hard- und Software welcher Hersteller kommt für dieses „Europol mobile office“ zum Einsatz?

Hierzu liegen der Bundesregierung keine Informationen vor.

b) Über wie viele „mobile offices“ verfügt Europol und wo sind diese in der Regel „stationiert“?

Hierzu liegen der Bundesregierung keine Informationen vor.

c) Nach welchen technischen Verfahren und Sicherheitsstandards werden Daten eines „mobile office“ übertragen?

Alle Sicherheitsstandards bei Europol richten sich nach dem Sicherheitshandbuch (Security Manual) von Europol.

d) Welche Kosten sind für die Ausrüstung von „mobile offices“ entstanden?

Im Jahr 2011 wurden für die „mobile offices“ 23 770 Euro verwendet. Der Haushaltsplan enthält keine weitere Aufschlüsselung der Kosten.

e) Worin besteht die Aufgabe der Europol-Bediensteten für die konkrete Handhabung dieses „mobile offices“?

Hierzu liegen der Bundesregierung keine Informationen vor.

f) Welche konkreten „vast improvements to its mobile office solution“ hat Europol wie im Review 2010 angegeben vorgenommen, die demnach eine „far greater flexibility and speed of deployment“ erlauben würden?

Die Stabilität des Systems wurde verbessert. Über Detailkenntnisse hierzu verfügt die Bundesregierung nicht.

4. Welche Rolle spielt die „powerful mobile office solution“ in der Koordination „polizeilicher Großlagen“?

Eine „powerful mobile office solution“ ist der Bundesregierung nicht bekannt. Soweit es sich um das „mobile office“ handeln sollte, können damit je nach Zugriffsberechtigung des anwendenden Europol-Beschäftigten Daten eingegeben und/oder recherchiert werden.

a) Welche Ereignisse im Bereich „internationally prominent sporting, economic, political or cultural gatherings“ wurden von Europol in den letzten fünf Jahren derart unterstützt, und worin bestand dessen Beitrag?

Hierzu liegen der Bundesregierung keine Informationen vor.

b) Auf welche Art und Weise arbeitet Europol hinsichtlich von „mobile offices“ mit Verfolgungsbehörden in Rumänien zusammen?

Hierzu liegen der Bundesregierung keine Informationen vor.

c) Welche Datenbanken und andere „technical equipment“ wurden hierfür in Rumänien installiert?

Hierzu liegen der Bundesregierung keine Informationen vor.

d) Wie ist die technische Ausrüstung eingebunden in andere internationale Kooperationsprojekte mit Rumänien, darunter auch die Southeast European Cooperative Initiative (SECI) bzw. das Southeast European Law Enforcement Center (SELEC)?

Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

5. Welche Hard- und Software welcher Firmen nutzt das von Deutschland bei Europol ins Leben gerufenen Mobile Competence Team (MCT) unter anderem zur Umsetzung des Vertrags von Prüm zum grenzüberschreitenden Datentausch, und wie wurde deren Beschaffung abgewickelt?

Worin besteht die Aufgabe des BKA sowie Rumänien und Österreichs innerhalb des MCT hinsichtlich der Nutzung von Soft- und Hardware, etwa als „Testplattform“ für „Pilottests“?

Bei dem Mobile Competence Team (MCT) handelt es sich um ein im Rahmen des EU ISEC-Förderprogramms eingerichteten Projekt unter deutscher Leitung. Aufgabe des MCT ist es, die noch nicht operativen Mitgliedstaaten bei der technischen Umsetzung der Prümer Beschlüsse im Hinblick auf den automatisierten Austausch von Fingerabdrücken und DNA zu unterstützen. Darüber hinaus soll das MCT die Einrichtung eines dauerhaften Prüm Helpdesk bei Europol unterstützen.

Die Projektleitung das MCT ist beim Bundeskriminalamt (BKA) in Wiesbaden angesiedelt. Rumänien und Österreich haben für die Laufzeit des Projekts je einen Experten für das MCT entsandt. Das MCT verwendet die im BKA eingesetzte Bürokommunikationssoftware (Betriebssystem Windows, Microsoft Office).

Im Rahmen des Projekts MCT wurde eine Erweiterung der Recherchekapazität für das bestehende deutsche Test AFIS (Automatische Fingerabdruck Identifikationssystem) beschafft. Das BKA stellt dieses Test AFIS während der Projektlaufzeit im Bedarfsfall als Testplattform den anderen Prüm-Teilnehmerstaaten zur Verfügung.

6. Über welche weitere „forensische Ausrüstung“ verfügt Europol, wie im Review 2010 angegeben?

Über das Review 2010 hinaus liegen der Bundesregierung keine weiteren Informationen vor.

a) Woraus besteht das im Europol-Review 2010 angeführte „forensic toolkit“ (UFED)?

Das „forensic toolkit“ besteht unter anderem aus Kartenlesern, einem Universal Forensic Extraction Device (UFED) und einer Kartenüberprüfungsdatenbank.

b) Wie viele „mobile phone scanners“ bevorratet die EU-Agentur, und um welche Produkte welcher Hersteller handelt es sich?

Hierzu liegen der Bundesregierung keine Informationen vor.

c) Nach welchen Kriterien kommen die „mobile phone scanners“ zum Einsatz?

Hierzu liegen der Bundesregierung keine Informationen vor. Die Bundesregierung weist darauf hin, dass Europol keine operativen Befugnisse hat.

d) Wie oft und in welchen Ländern wurden die „mobile phone scanners“ von Europol bereits genutzt?

Hierzu liegen der Bundesregierung keine Informationen vor.

e) An welchen gemeinsamen Operationen haben deutsche Behörden teilgenommen, innerhalb derer „mobile phone scanners“ von Europol eingesetzt wurden?

Hierüber werden keine Statistiken geführt.

7. Welches Werkzeug zur Analyse Sozialer Netzwerke (SNA tool), welcher Hersteller ist von Europol konkret gemeint, das bei der „Operation Most“ zum Einsatz kam?

Nach Kenntnis der Bundesregierung handelt es sich bei SNA nicht um ein Analysetool für Soziale Netzwerke. Vielmehr sollen diese Werkzeuge die visuelle Darstellung von Beziehungsgeflechten der bei Europol vorhandenen Daten unterstützen. Weitere Information liegen der Bundesregierung nicht vor.

a) Über welche Funktionalitäten verfügt dieses „SNA tool“, und welche mathematischen Algorithmen kommen dabei zur Anwendung?

Hierzu liegen der Bundesregierung keine Informationen vor.

b) Auf welche Datenbanken greift das „SNA tool“ im Regel- und im Einzelfall zu?

Hierzu liegen der Bundesregierung keine Informationen vor.

c) Auf welche Art und Weise hat das „SNA tool“ bei der „Operation Most“ dafür gesorgt, 25 Verdächtige aus einer Million mitgeschnittenen Telefongesprächen zu extrahieren?

Hierzu liegen der Bundesregierung keine Informationen vor.

d) Wie ist die Funktionsfähigkeit dieses „SNA tools“ getestet worden?

Hierzu liegen der Bundesregierung keine Informationen vor.

e) Welche anderen Anbieter ähnlicher Software wurden vor oder nach der Einführung des „SNA tools“ hinsichtlich einer Verbesserung, Evaluierung oder Anschaffung anderer Produkte eingebunden?

Hierzu liegen der Bundesregierung keine Informationen vor.

f) Wie wird sichergestellt, dass die aufgrund der Analyse des „SNA tools“ Verhafteten nicht durch einen Softwarefehler ins Visier der festnehmenden Behörden in Polen gerieten?

Im Rahmen strafprozessualer Maßnahmen bzw. in Strafverfahren sollte generell eine Prüfung der Beweislage erfolgen. Über die Verwendung von Informationen aus Europol-Analyseberichten durch die zuständigen polnischen Strafverfolgungsbehörden liegen der Bundesregierung keine Informationen vor.

g) Wie wird sichergestellt, dass die derart erlangten Erkenntnisse vor Gericht verwertet werden können?

Die Verwertbarkeitsprüfung sollte aus rechtlicher Sicht Teil des Gerichtsverfahrens sein.

h) Wie oft wurde das „SNA tool“ von Europol bereits eingesetzt, und bei welchen Operationen waren Behörden der Bundesregierung daran beteiligt?

Hierzu liegen der Bundesregierung keine Informationen vor.

i) In welchen internationalen Arbeitsgruppen erörtert Europol operative oder technische Aspekte hinsichtlich des Einsatzes von „SNA tools“?

Es sind der Bundesregierung weder interne Europol-Arbeitsgruppen noch internationale Arbeitsgruppen bekannt, in denen Europol operative oder technische Aspekte hinsichtlich des Einsatzes von SNA Werkzeugen erörtert oder zur Diskussion gestellt hat.

8. Auf welche deutschen Informationssysteme haben die Agenturen Europol und Eurojust (Einheit für justizielle Zusammenarbeit der Europäischen Union – EUROJUST) lesenden oder schreibenden Zugriff?

Die Agenturen Europol und Eurojust haben keinen lesenden oder schreibenden Zugriff auf deutsche Informationssysteme.

a) Wie ist geregelt, inwieweit die hierüber erlangten Informationen mit forensischen Methoden Europols ausgewertet werden dürfen?

Es wird auf die Antwort zu Frage 8 verwiesen.

b) Wie wird ausgeschlossen, dass die Daten ohne Wissen deutscher Behörden in Ermittlungen von Europol verwendet werden?

Es wird auf die Antwort zu Frage 8 verwiesen.

c) Welchen Inhalt hatte das „Proposal on Social Media Communication guidelines for law enforcement authorities“, das von der früheren ungarischen Ratspräsidentschaft vorgestellt wurde?

Das „Proposal on Social Media Communication guidelines for law enforcement authorities“ enthält einen Vorschlag der ungarischen Ratspräsidentschaft zu Leitlinien für die Nutzung sozialer Netzwerke durch Strafverfolgungsbehörden und ihrer Mitarbeiter. Thematisiert werden darin sowohl allgemeine Fragestellungen z. B. bezüglich der Social-Media-Kommunikationspolitik von Strafverfolgungsbehörden, des Austausches von best practices unter den Mitgliedstaaten oder bezüglich der Sensibilisierung und Fortbildung von Mitarbeitern der Strafverfolgungsbehörden zu Risiken sozialer Netzwerke und notwendiger Schutzmaßnahmen. Daneben enthält der Vorschlag konkrete Empfehlungen an die Strafverfolgungsbehörden (die sogenannten goldenen Regeln), die das Kommunikationsverhalten und die Nutzung von Social Media Tools betreffen (z. B. Fragen der Vertraulichkeit und des Geheimschutzes, der Wahrung parteipolitischer Neutralität, des Disziplinarrechts, des Datenschutzrechts oder des Verhältnisses privater und dienstlicher Nutzung).

Die ungarische Ratspräsidentschaft stellte das Dokument zunächst nur zur Kenntnisnahme vor.

9. Worin besteht die Aufgabe des „Computer Forensic Networks“ bei Europol?

Hierbei geht es um den Aufbau von Kompetenzen hinsichtlich der Auswertung digitalisierter Informationen. Es liegen keine über die im Review 2010 hinausgehenden Informationen vor.

a) Welche Anwendung ist gemeint, die Europol im Review 2010 mit „state-of-the-art facility to extract and analyse crime-related information from digitised data“ bewirbt?

Hierzu liegen der Bundesregierung keine Informationen vor.

b) Welche Produkte welcher Hersteller werden hierfür eingesetzt?

Hierzu liegen der Bundesregierung keine Informationen vor.

c) Wie hat Europol bewerkstelligt, „dramatic improvements in the quantity of data that can be processed“ vorzunehmen?

Hierzu liegen der Bundesregierung keine Informationen vor.

d) Worin besteht das „expert-operated mobile toolkit for computer data forensics“, und über welche Funktionalitäten verfügt die Anwendung?

Hierzu liegen der Bundesregierung keine Informationen vor.

10. Worin besteht die Arbeit der „Cross-Border Surveillance Working Group“ (CSW), deren Mitglied Europol ist?

Die Cross Border Surveillance Working Group (CSW) verfolgt in Einzelprojekten sowie regelmäßigen Treffen von Teilnehmern europäischer Länder eine Stärkung der bi- und multilateralen Kontakte sowie Vermittlung von Ausbildungs- sowie technischen Inhalten.

Die Projekte befassen sich mit:

- Hospitationen im Bereich Observationstechnik und -taktik,
- Ausbildungsangeboten in einzelnen Spezialbereichen,
- Verbesserung der Zusammenarbeit durch Übungen in Echtlagen sowie „Table-Top-Exercises“,
- Aufbau einer internationalen Informations- und Kommunikationsplattform bei EUROPOL für Belange der Observationseinheiten (in Arbeit, noch kein Wirkbetrieb). Die Projekte werden bedarfsorientiert ausgerichtet und sind somit nicht abschließend.

a) Seit wann existiert die CSW, und welche Behörden oder sonstigen Stellen welcher Länder nehmen daran teil?

Am 19. und 20. Mai 2005 fand in London die erste Sitzung der „Cross-Border Surveilance Working Group“ statt, an der Vertreter aus dem Bereich der Mobilen Einsatzkommandos (oder vergleichbare Einheiten) aus Großbritannien, Niederlande, Belgien, Schweiz, Österreich, Spanien und Deutschland teilgenommen haben. Inzwischen sind Vertreter von zwölf EU-Mitgliedstaaten sowie der Schweiz an der Working Group beteiligt. Europol entsendet eine Mitarbeiterin zu dieser Arbeitsgruppe. Es handelt sich hierbei um eine informelle Arbeitsgruppe dieser Mitgliedstaaten zu einem Spezialgebiet. Zu den unregelmäßig tagenden Besprechungen entsendet das Bundeskriminalamt einen Vertreter.

b) Auf wessen Veranlassung wurde die Gruppe gegründet?

Hierzu liegen der Bundesregierung keine Informationen vor.

c) Welche Themen bzw. konkreten Überwachungswerkzeuge standen auf den Treffen der letzten fünf Jahre jeweils auf der Tagesordnung?

Ziel der CSW war und ist es, ein Forum zum informellen Informationsaustausch zu schaffen, bei dem Sachbearbeiter wie auch Führungskräfte gleichermaßen beteiligt sein sollen. Hierbei sollen im Rahmen einer vertrauensvollen Zusammenarbeit auf internationaler Ebene Erfahrungen zu Themen wie Taktik der Einsatzbewältigung, technische Einsatzmittel, Aus- und Fortbildung sowie internationale Zusammenarbeit besprochen werden.

d) Welche Methoden zur verdeckten Beobachtung von Personen oder Sachen hat Europol entwickelt bzw. setzt diese ein?

Hierzu liegen der Bundesregierung keine Informationen vor.

11. Welche Soft- und Hardware welcher Hersteller wird von der EU-Agentur FRONTEX (etwa zur Fallbearbeitung) eingesetzt und wie wurde ihre Beschaffung geregelt?

Inwieweit neben Microsoft Office-Produkten, Chias-Verschlüsselungssoftware und nicht spezifizierbare Software zur Bearbeitung/Erstellung von PDF-Dokumenten weitere Software genutzt wird, ist der Bundesregierung nicht bekannt.

a) Welche Software welcher Hersteller wird von der „Frontex Situation Center Unit“ genutzt, um „Risikoanalysen“ oder Lageberichte zu verfassen?

Nach hiesigem Kenntnisstand werden vom Frontex Situation Centre zur Erstellung von Lageberichten Office-Anwendungen genutzt. Risikoanalysen werden nicht vom Frontex Situation Centre erstellt.

b) Welche Software welcher Hersteller liegt dem „Frontex One-Stop-Shop web portal“ (FOSS) zugrunde?

Beim Frontex-One-Stop-Shop (FOSS) handelt es sich vorrangig um ein Filesharingsystem. Dem Impressum dieser Webseite ist zu entnehmen, dass das Joint Research Centre der EU zumindest an der Entwicklung beteiligt war. Weitere Einzelheiten sind der Bundesregierung nicht bekannt.

c) Welche Behörden der EU-Mitgliedstaaten sind bereits an das FOSS angebunden bzw. sollen zukünftig angeschlossen werden?

Am FOSS sind grundsätzlich die Grenzpolizeibehörden der Mitgliedstaaten angeschlossen.

d) Welche Software welcher Hersteller liegen dem „Frontex Media Monitor“ zugrunde und welche technische Spezifikationen erfüllt die Anwendung?

Nach hier vorliegenden Informationen wurde das Frontex Media Monitor System durch das Joint Research Centre der EU in Zusammenarbeit mit der Universität Helsinki und Unterstützung von Frontex entwickelt. Bei dem System handelt es sich um eine webbasierte Anwendung zur Sammlung und Darstellung von Informationen und Nachrichten der Weltpresse.

e) Auf welcher Software welcher Hersteller basiert die „Joint Operations Reporting Application“ (JORA), und welche technische Spezifikationen erfüllt die Anwendung?

Bei JORA handelt es sich um eine web- und flashbasierte Anwendung zur Übermittlung von nicht personenbezogenen Vorgangs-/Lagedaten sowie deren anschließende Visualisierung. Bei der Entwicklung war die polnische Firma ASSECO beteiligt. Eine Sicherheitsüberprüfung durch das Bundesamt für Sicherheit in der Informationstechnik verlief ohne Auffälligkeiten.

f) Wie sind Schreib- und Leserechte für beteiligte Stellen und Behörden der Mitgliedstaaten innerhalb des FOSS, des „Frontex Media Monitors“ und des JORA geregelt?

FOSS – Frontex verfügt über Schreib- und Leserechte, die angebundenen Nutzer haben lediglich Leserechte.

JORA – Das System befindet sich noch nicht im Wirkbetrieb, Schreib- und Leserechte sollen einzelfallbezogen und -angepasst an die Nutzer vergeben werden.

Frontex Media Monitor System – Da es sich um eine Anwendung ähnlich einer Suchmaschine handelt, ist die Vergabe von Schreib- und Leserechten nicht vorgesehen.

12. Welche Überlegungen wurden von der Bundesregierung bislang zur Beteiligung am „Common Pre-Frontier Intelligence Picture“ (CPIP) angestellt, mit dem der „vorgelagerte Grenzbereich“ innerhalb von EUROSUR überwacht werden soll?

Es liegt erst ein Vorschlag der Kommission über die Errichtung von EUROSUR vor, der bislang noch nicht in den zuständigen Ratsgremien beraten wurde. Eine innerhalb der Bundesregierung abgestimmte Haltung gibt es daher zu diesem Vorschlag noch nicht.

Aus deutscher Sicht könnte es aber sinnvoll sein, Informationen aus dem vorgelagerten Grenzbereich für die strategische Risikobewertung von Migrationsbewegungen zu nutzen. Diesbezüglich könnten z. B. die in Drittstaaten entsandten Verbindungsbeamten der Mitgliedstaaten sowie zukünftig auch die FRONTEX-eigenen Verbindungsbeamten entsprechende Beiträge leisten.

a) Wo könnte ein deutsches „National Coordination Centre“ (NCC) im Rahmen von EUROSUR angesiedelt werden, und welche Überlegungen wurden hierzu von wem bereits angestellt?

Vorbehaltlich weiterer Überlegungen, könnte der Sitz eines deutschen NCC im Rahmen von EUROSUR im Bundespolizeipräsidium angesiedelt werden. Die spezifische Aufgabe der Seeaußengrenzüberwachung könnte im Gemeinsamen Lagezentrum See in Cuxhaven angebunden werden.

b) Welche Aufgaben würde ein deutsches NCC übernehmen?

Die möglichen Aufgaben eines NCC im Rahmen von EUROSUR ergeben sich aus Artikel 5 des Vorschlags für eine EUROSUR-Verordnung (KOM (2011) 873 vom 12. Dezember 2011).

Nach diesem noch zu prüfenden Vorschlag stellen sich die wesentlichen Aufgaben wie folgt dar:

- Informationsaustausch mit den anderen NCC;
- Beitrag zu einem effizienten Personal- und Mitteleinsatz;
- Fortschreibung und ständige Aktualisierung des nationalen Lagebildes;
- Unterstützung der Planung/Umsetzung nationaler Grenzüberwachungsmaßnahmen;
- Soweit vorhanden: Betreiben nationaler Grenzüberwachungssysteme gemäß innerstaatlichem Recht;
- Regelmäßige Evaluierung nationaler Grenzüberwachungsmaßnahmen;
- Koordination operativer Maßnahmen mit anderen Mitgliedstaaten.

13. Inwieweit nutzt Deutschland hinsichtlich des „Europäischen Strafregisterinformationssystems“ (ECRIS) Anwendungen der „Interactive Listening and CONNecting“ (iLiCONN), und um welche Soft- und Hardware welcher Hersteller handelt es sich dabei konkret?

Zum jetzigen Zeitpunkt wird iLICONN von Behörden des Bundes nicht genutzt.

Die Automatisierung im Rahmen des Europäischen Strafregisterinformationssystems (ECRIS) erfasst nur die automatisierte Datenübermittlung zwischen den zentralen Strafregisterbehörden. Ein Zugang zu den nationalen Strafregistern (lesend oder schreibend) ist damit nicht verbunden. In Deutschland eingehende Strafnachrichten oder Auskunftsersuchen werden nach Eingang manuell bearbeitet.

Es ist lediglich beabsichtigt, die von ILICONN für die Europäische Kommission entwickelte ECRIS-Referenzimplementierung für die künftige Kommunikation mit den Partnern im ECRIS-Verbund zu nutzen, und zwar insbesondere den Webservice für die Außenkommunikation.

a) Auf welche Datenbanken greift iLiCONN zu, bzw. welche sonstigen Datensätze werden verarbeitet?

Auf welche Datenbanken iLICONN generell zugreift, ist nicht bekannt. Auf deutsche Datenbanken im Zusammenhang mit ECRIS jedoch nicht.

b) Wie wurde die Anwendung zuvor getestet, und welche Kriterien zur Qualitätssicherungen mussten erfüllt werden?

Nach Aussage von iLICONN wird die ECRIS-Referenzimplementierung bei iLICONN und zusammen mit der EU-Kommission getestet. Die Nationalstaaten sind „nur“ Nutzer und nicht für die Qualitätssicherung verantwortlich.

c) Haben deutsche Behörden die Möglichkeit, den Quellcode verwendeter Software einzusehen oder anderweitig zu prüfen?

Behörden des Bundes haben keine Möglichkeit, den Quellcode der ECRIS-Referenzimplementierung einzusehen und zu prüfen.

14. Inwieweit ist das „European Network of Law Enforcement Technology Services“ (ENLETS) mit der Durchführung, Erörterung oder Evaluierung von Maßnahmen zur Kommunikationsüberwachung befasst?

Das unter französischer EU-Präsidentschaft 2008 gegründete Netzwerk Enlets hat zum Ziel, den Strafverfolgungsbehörden die Möglichkeit zum informellen Erfahrungsaustausch zu geben und sie in die Lage zu versetzen, sich an Sicherheitsforschung zu beteiligen und von dieser zu profitieren. Das Netzwerk selbst ist nicht mit der Durchführung und Evaluierung von Maßnahmen zur Kommunikationsüberwachung befasst. Ob es solche Maßnahmen im Rahmen seiner Treffen erörtert hat, ist der Bundesregierung nicht bekannt.

a) Welche Treffen mit welchen Inhalten haben seit Gründung des ENLETS stattgefunden?

Das Gründungstreffen des Netzwerkes fand im September 2008 unter französischer Präsidentschaft in Brüssel statt. Bei dem Treffen ging es neben einem allgemeinen Erfahrungsaustausch um die Ziele des Netzwerkes und die Identifizierung von Kontaktpunkten. Das zweite Treffen in Prag im April 2009 befasste sich schwerpunktmäßig mit Regeln der Zusammenarbeit im Enlets-Netzwerk und der Organisation der Treffen. Beim dritten Treffen in Stockholm im Oktober 2009 ging es vor allem um die Schaffung einer elektronischen Plattform für einen Informationsaustausch. Das vierte Treffen im Februar 2010 befasste sich mit der besseren Einbeziehung der Europäischen Kommission in die Arbeit des Netzwerkes. Ein weiteres Treffen fand im September 2010 am Rande der European Research Conference in Oostende statt. Beim letzten Treffen im September 2011 in Warschau ging es neben einem allgemeinen Erfahrungsaustausch, der bei jedem Treffen auf der Agenda steht, um eine Erläuterung der Evaluierungskriterien und des Evaluierungsprozesses für Sicherheitsforschungsprojekte im Rahmen des 7. EU-Forschungsrahmenprogramms.

b) Welche Technologien werden derzeit innerhalb von ENLETS behandelt?

Das Netzwerk Enlets dient vor allem dem Erfahrungs- und Informationsaustausch. Eine weitergehende „Behandlung“ von Technologien findet nicht statt.

c) Welche Angaben macht die Bundesregierung hinsichtlich des Registers zu „Sicherheitstechnologie“, das innerhalb von ENLETS angelegt werden soll?

Ein „Register zur Sicherheitstechnologie“ ist der Bundesregierung nicht bekannt.

d) Welche Stelle wird von deutschen Behörden als „ENLETS National Contact Point“ benannt?

Die Bundesregierung hat einen Mitarbeiter der Deutschen Hochschule der Polizei in Münster als Nationale Kontaktstelle benannt.

e) Wie arbeiten andere EU-Agenturen innerhalb von ENLETS mit?

An den Enlets-Treffen haben neben Europol teilweise auch FRONTEX, die Research Executive Agency, das Joint Research Centre und die Kommission teilgenommen. Ob über die Teilnahme an Konferenzen hinaus eine Zusammenarbeit besteht, kann die Bundesregierung nicht sagen.

f) Mit welchen Kapazitäten vor allem im IT-Bereich arbeitet die Polizeiagentur Europol in ENLETS mit?

Europol wurde über die Ratsarbeitsgruppe Strafverfolgung gebeten, Enlets durch eine einzurichtende IT-Plattform für Experten zu unterstützen. In einer „Europol Platform for Experts“ können zum Beispiel eine Liste nationaler Kontaktpunkte oder Referenzdokumente (Schulungsmaterial, Rechtstexte, Richtlinien, Durchführungsvereinbarungen, etc.) bereit gehalten werden; ein Austausch personenbezogener Daten erfolgt nicht.

g) Inwieweit sind Firmen der Rüstungs- und Softwareindustrie in die Arbeit von ENLETS eingebunden?

Der Bundesregierung ist eine Einbindung von Firmen der Rüstungs- und Softwareindustrie in die Arbeit von Enlets nicht bekannt.

h) Welche Zusammenarbeit pflegt ENLETS mit Instituten, Hochschulen oder sonstigen Einrichtungen der EU-Mitgliedstaaten?

Das ist der Bundesregierung nicht bekannt.

i) Inwieweit berücksichtigt ENLETS laufende EU-Forschungsvorhaben im Bereich der Sicherheits- und Überwachungstechnik?

Das Netzwerk Enlets dient vor allem dem Erfahrungs- und Informationsaustausch. Hierbei sind selbstverständlich neueste Entwicklungen und laufende Forschungsvorhaben zu berücksichtigen.

j) Was wurde anlässlich des Vortrags von dem Wissenschaftler Andrzej Dziech von der AGH University of Science and Technology in Krakau (Polen) bei einem der jüngsten Treffen von ENLETS besprochen, und welche weiteren Verabredungen wurden getroffen?

Die Bundesregierung war beim letzten Enlets-Treffen in Warschau nicht vertreten. Sie hat deswegen keine Kenntnis darüber, was anlässlich eines Vortrags von Andrzej Dziech besprochen und welche Verabredungen getroffen wurden.



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333